Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 19 novembre 2001
N° CERTA-2001-ALE-015

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation massive d'une ancienne vulnérabilité de SSH

Gestion du document

Référence	CERTA-2001-ALE-015
Titre	Exploitation massive d'une ancienne vulnérabilité de SSH
Date de la première version	19 novembre 2001
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Compromission du système.

2 Systèmes affectés

Tous les systèmes utilisant :

- SSH-1.5-1.2.24 à SSH-1.5-1.2.31,
- SSH-1.5-OpenSSH-1.2 à SSH-1.5-OpenSSH-1.2.3,
- SSH-1.99-2.0.11 à SSH-1.99-2.0.13 avec la fonctionnalité `fallback` activée,
- SSH-1.99-2.1.0.p12 avec la fonctionnalité `fallback` activée,
- SSH-1.99-2.1.0 avec la fonctionnalité `fallback` activée,
- SSH-1.99-2.2.0 avec la fonctionnalité `fallback` activée,
- SSH-1.99-2.3.0 avec la fonctionnalité `fallback` activée,
- SSH-1.99-2.4.0 avec la fonctionnalité `fallback` activée,
- SSH-1.99-3.0.0 avec la fonctionnalité `fallback` activée,
- SSH-1.99-3.0.1 avec la fonctionnalité `fallback` activée,

– SSH-1.99-OpenSSH-2.1,
– SSH-1.99-OpenSSH-2.1.1,
– SSH-1.99-OpenSSH-2.2.0,
– SSH-1.99-OpenSSH-2.2.0p1,
– SSH-2.0-2.3.0 avec la fonctionnalité `fallback` activée,
– SSH-2.0-2.4.0 avec la fonctionnalité `fallback` activée,
– SSH-2.0-3.0.0 avec la fonctionnalité `fallback` activée,
– SSH-2.0-3.0.1 avec la fonctionnalité `fallback` activée,

D'autres versions de SSH sont peut-être vulnérables.

3 Résumé

La faille décrite dans l'avis CERTA-2001-AVI-017 est exploitée pour compromettre les systèmes.

4 Description

SSH est un service permettant un accès distant via un tunnel chiffré. Ce service peut être utilisé pour administrer, à moindre risque, des machines à distance.

La faille de sécurité de SSH décrite dans l'avis CERTA-2001-AVI-017 est actuellement massivement exploitée, compromettant ainsi de nombreux systèmes.

Certaines versions de SSH, apparemment non vulnérables, deviennent vulnérables lorsque la fonctionnalité `fallback` est activée. En effet, cette fonctionnalité, mise en oeuvre sur une version non vulnérable, fait appel à une version de SSH1 vulnérable.

Les attaques par SSH laissent des traces assez significatives dans les fichiers journaux (par exemple `/var/log/secure`). Voici un exemple de ces traces :

```
Nov 19 11:00:00 victime sshd[pid]: log: Connection from attaquant port numero_de_port
Nov 19 11:00:04 victime sshd[pid+1]: log: Connection from attaquant port numero_de_po
Nov 19 11:00:07 victime sshd[pid+2]: log: Connection from attaquant port numero_de_po
Nov 19 11:00:11 victime sshd[pid+3]: log: Connection from attaquant port numero_de_po
Nov 19 11:00:16 victime sshd[pid+4]: log: Connection from attaquant port numero_de_po
Nov 19 11:00:16 victime sshd[pid+4]: fatal: Local: crc32 compensation attack:
network attack detected
```

victime : Nom de la machine victime
pid : Numéro de processus de sshd, incrémenté à chaque nouvelle connexion
attaquant : Nom de machine ou adresse IP attaquante
numero_de_port : Numéro de port source, incrémenté pendant l'attaque

5 Contournement provisoire

– Mettre à jour la version de SSH,
– ne pas utiliser la fonctionnalité `fallback`,
– mettre des règles de filtrage au niveau du garde-barrière pour bloquer le port 22/tcp (ou le port sur lequel SSH est en écoute) pour les machines non-autorisées,
– si le service SSH est lancé par `tcp-wrapper` (tcpd) dans `inetd`, configurer les fichiers `/etc/hosts.allow` et `/etc/hosts.deny` pour spécifier les machines autorisées à utiliser ce service,
– si le service SSH est lancé par `xinetd`, modifier le fichier `/etc/xinetd.conf` pour spécifier les machines autorisées à utiliser ce service.

6 Solution

Se référer au bulletin de sécurité CERTA-2001-AVI-017 du 12 février 2001.

7 Contournement provisoire

Analyse de Dave Dittrich :
http://staff.washington.edu/dittrich/misc/ssh-analysis.txt

Gestion détaillée du document

19 novembre 2001 version initiale.